

Objective

- **Objective**

***To understand the “Advance Persistent Attack” on
Country’s Critical Infrastructure***

Index

- **Key Learning**

- Overview
- What is Critical Information Infrastructure
- Advance Persistent Attacks on Power Sector – Cases
- What is Advance Persistent threat
- Steps of an Advance Persistent Attack
- What it is and What it is not
- How to prevent an organization from Advance Persistent threat
- Conclusion



Overview

Overview

- *The world is changing..*




Overview

- *The world is changing..*



Overview

- 
- *The world is changing..*
 - Killing Economy is better prospect than killing people
 - Hit the Advantageous realm (Critical Infrastructure) of the non friendly nation
 - Low cost with better result



What is Critical Information Infrastructure

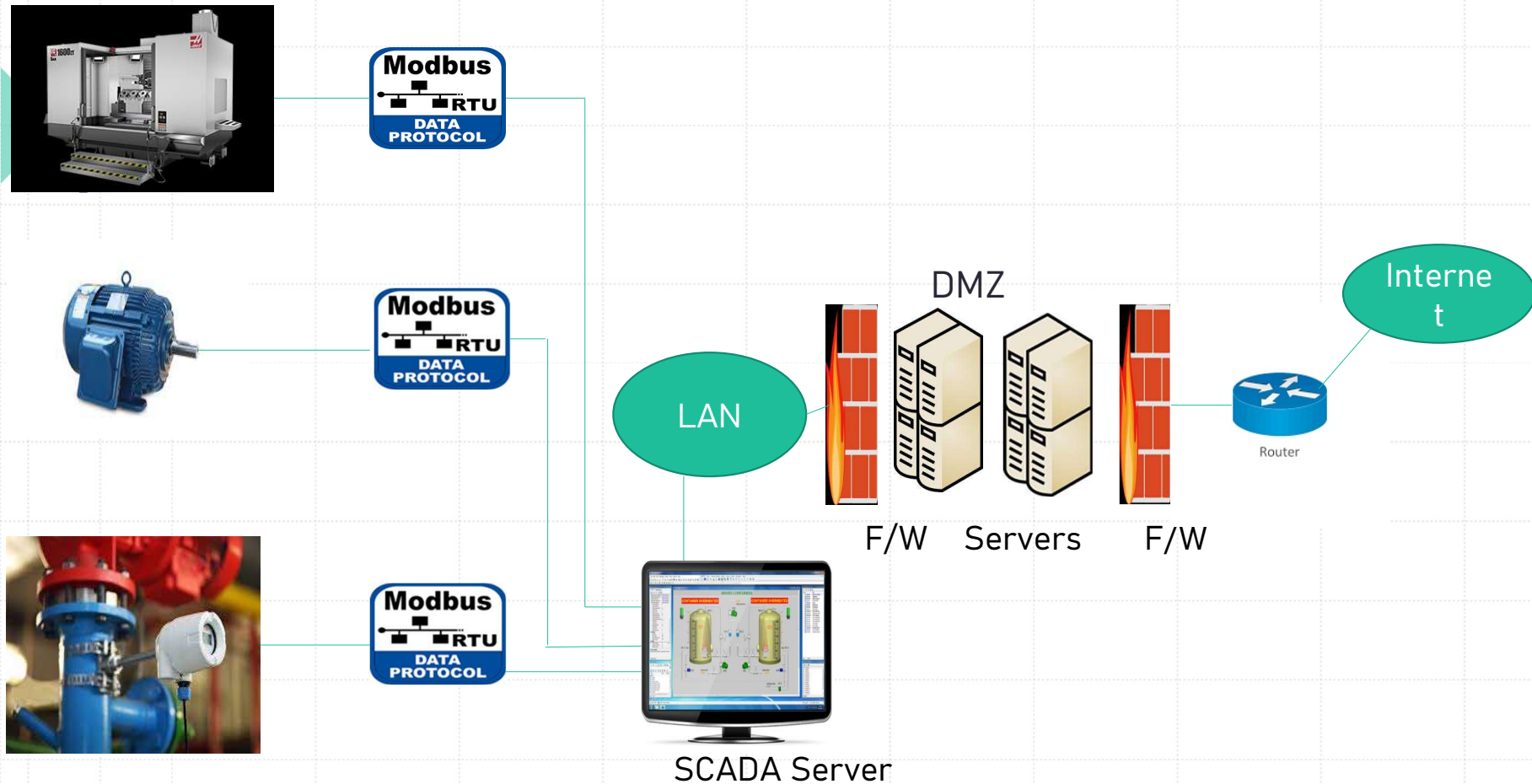
Critical Infrastructure Industries (CII)

- *Critical Information Infrastructure" means the computer resource, the incapacitation or destruction of which , shall have debilitating impact on national security, economy, public health or safety. (Sec. 70, IT Act 2008)*
- *Power, Oil & Gas, Petroleum, Road & Railways, Defense, Telecommunications, Banking & Finance, Water etc....*

Critical Infrastructure Industries (CII)

- *Most of the Critical Infrastructure industries equipped with automated operation by using SCADA (Supervisory Control and Data Acquisition System) and ICS (Industrial Control System) command and controlled by the programmed Computers.*
- *Any Malicious entry into these systems may tamper the information to provide wrong command to SCADA and ICS in intention to collapse the Critical Infrastructure industry and hence the country's economy.*

Critical Infrastructure Industries (CII)



Case Study



Advance Persistent Attack on Power Sector – Cases

Case Study-1

- Iran as Target – Bushehr Nuclear Power Plant & Natanz Nuclear facility was forcibly shutdown by the US-Israel worm StuxNet in the year 2010-2011.
- The attacks seem designed to force a change in the centrifuge's rotor speed, first raising the speed and then lowering it, likely with the intention of inducing excessive vibrations or distortions that would destroy the centrifuge.
- According to the Israeli newspaper Haaretz, in September 2010 experts on Iran and computer security specialists were increasingly convinced that StuxNet was meant "to sabotage the uranium enrichment facility at Natanz – where the centrifuge operational capacity had dropped over the past year by 30 percent

Case Study-2

- In the year 2013, an Attack was launched on turbine control system on Germany's Gundremmingen Plant.
- It took 5 years for the hackers to launch the attack. Phishing emails sent to the employees for the stealing of the user credentials to enter into the network of the company.
- Hackers used W32.Ramnit and Conficker malware and then used Pen Drive to poison turbine control system and result of that Plant was offline for three weeks.
- Why this happened: Pen Drives allowed in power control system. Used USB to charge mobiles in the power control systems. Security staff lack to monitor the activity happens .

Case Study-3

- In the year 2013, 17 Number of Electric Transformers worth \$15 Million damaged of USAs Pacific Gas & Electric Company (Metcalf Transmission Substation at Coyote, California)
- The company was unable to deliver power to the customers, till rerouting being done.
- Time taken by Hackers: 01 year to plan and operation completed in three hours.
- Weak Peripheral Security practices by the company and no IT Monitoring System was available with the company.

APT



*What is Advance Persistent Threat (APT)
Attack*

What it is

Advance Persistent Attacks (APT) or Zero Day Attack is a prolonged and targeted cyber attack in which an hacker gains access to a network and remains undetected for an extended period of time.

This attack is serious threat to an organization's intellectual property, financial assets and reputation and APT also target country's critical infrastructure like power, railway, telecom and government's sensitive information related to defense, economics, strategies. The APT used by

1. Terrorist
2. Non Friendly Nation
3. Non State Actors
4. Competitor Organization
5. An Individual with malicious intentions

What it is

In **Advance Persistent Attacks or Zero Day Attack**, a bot or malware is placed in the organization's CII by a hacker sitting in a remote country usually from a non friendly nation.

The bot or malware do the destruction to the CII by taking the command from the hackers.

Hackers are either government employees of the non friendly nation or hired by the government for the such operation.

Cost of one APT attack = Cost to the army for 35 years of service of two Colonel level Rank Solders + 20 years pension their on + Arms and ammunition used by them in their total service.

Damage by an APT attack may be > maximum up to 1/20 of the economy of the country.

APT



Steps of a Advance Persistent Attack

Define Target



This industry of this nation...



[Back](#)

Find and Organize Accomplices

Plants in these states...



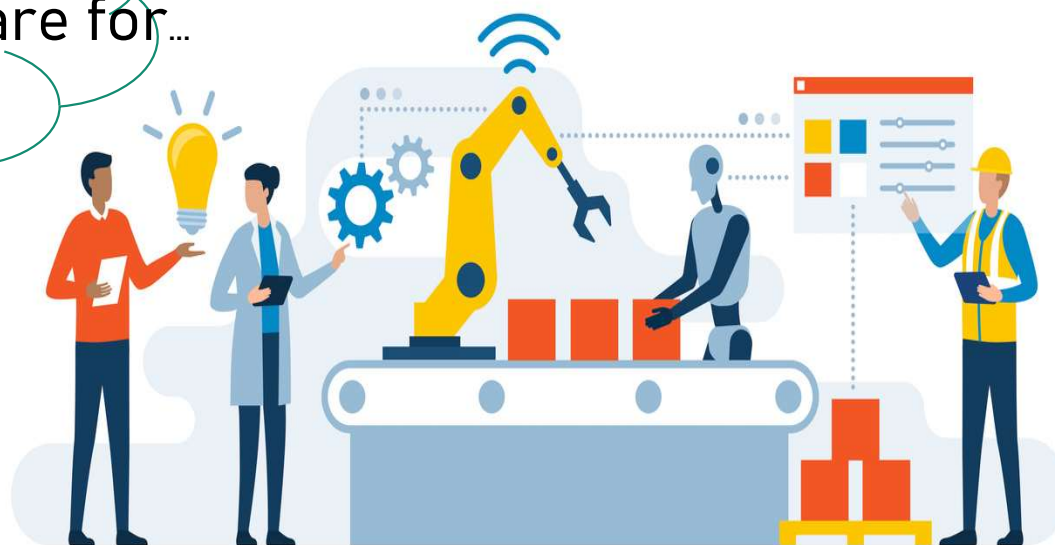
Research on Target

When and how to enter...



Build or Acquire Tools

Develop this malware for...



Development of malware as per need

Malware

Malware or bot (is a malicious software)
will be the local agent of hackers and
operate as per command from the hackers



Test on Detection

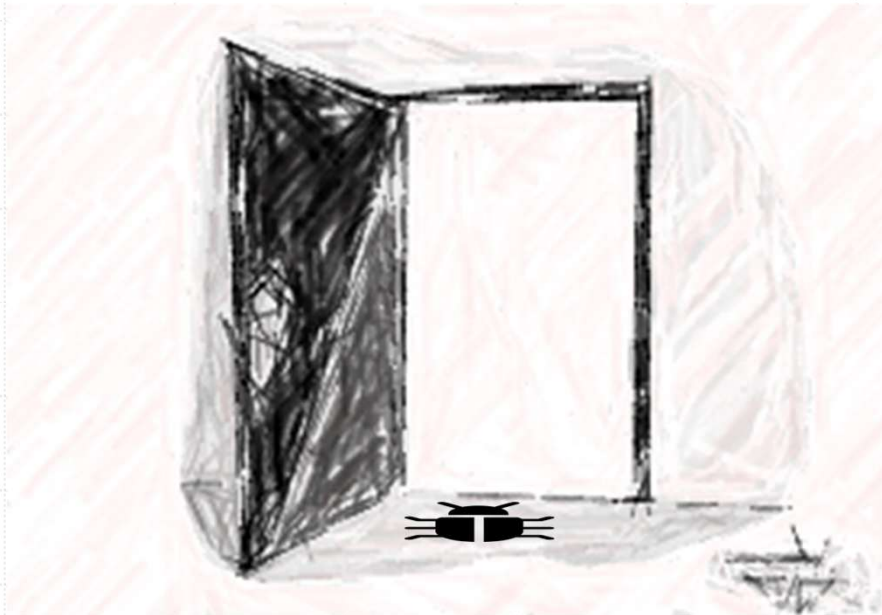


Test the malware

Deployment



Initial Intrusion



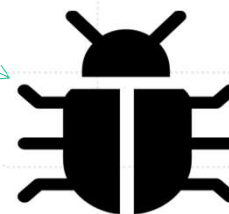
[Back](#)

Outbound Connection Initiated



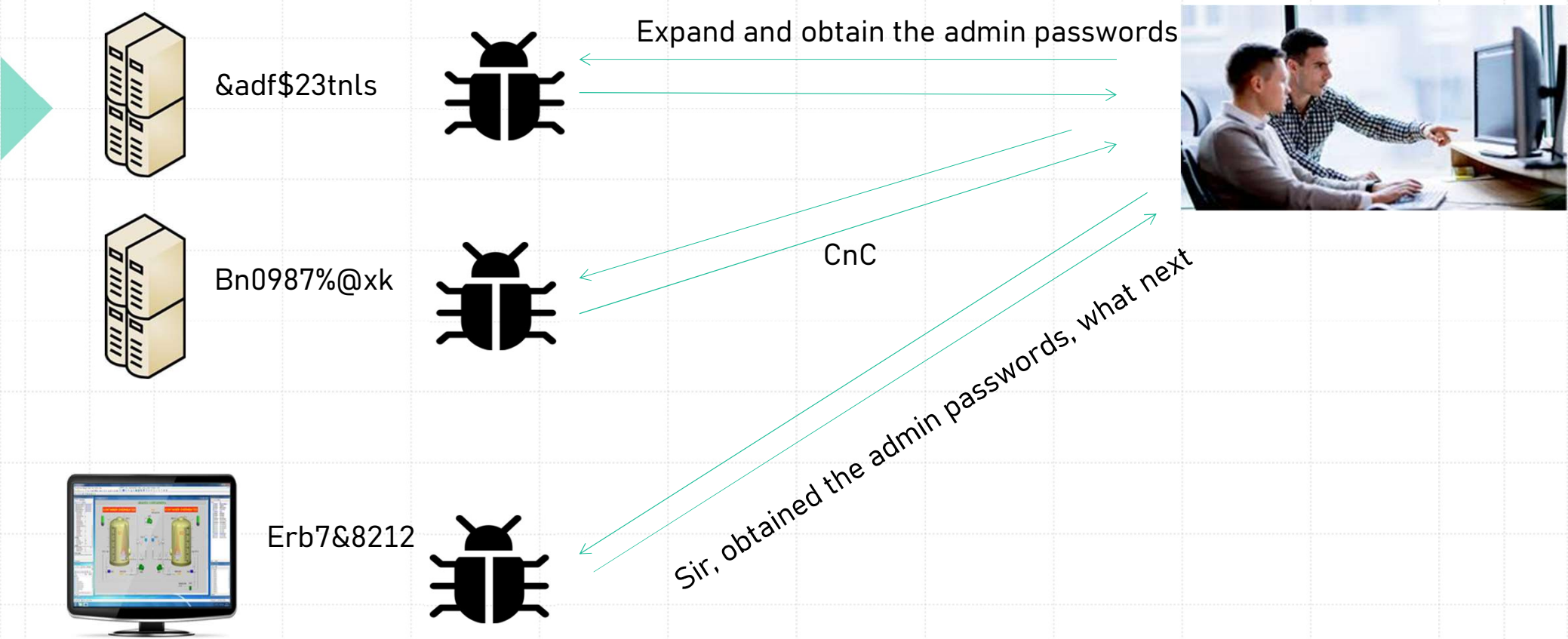
Sir, I reached here, Please give me the direction

Good, Wait for the Command



Command & Control

Expand Excess and Obtained Credentials of the Important Servers



Strengthen foothold



[Back](#)

Manoeuvre Data, Change Command, Destroy System



Send us plant parameters configured in the SCADA Server

Please accept the demanded parameter

Change boiler operating temperature From 102°C to 904°C & Pressure from 200 Pascal to 879 Pascal



	Mode R1
ie boiler outlet, °C	99.5
iler outlet	269.5
ler outlet, %	86.8
°C	36.1
'the air heaters	87.45
	156
	1.69
	10.94/8.68
	206
	1.415
	No. 4

Back

Manoeuvre Data, Change Command, Destroy System



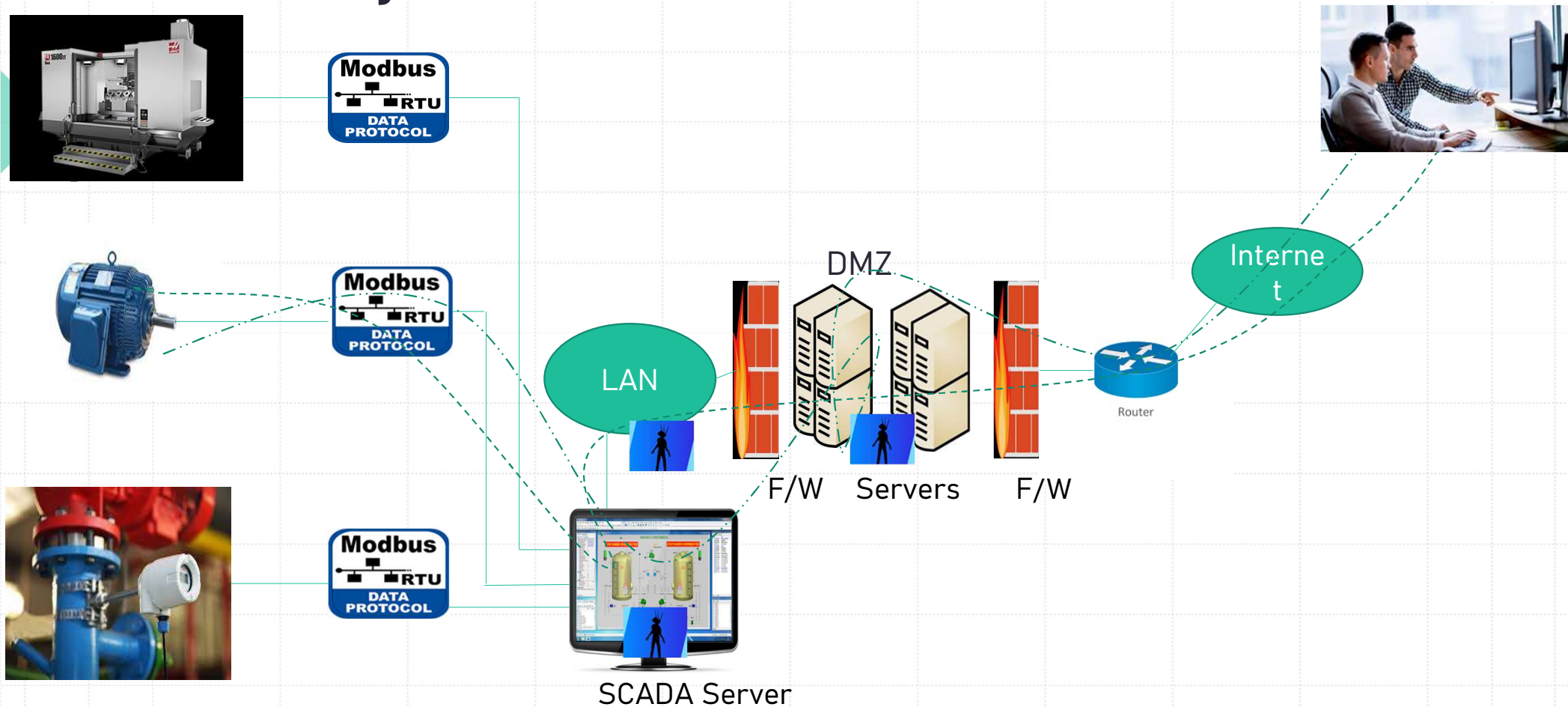
[Back](#)


Cover tracks & remain undetected



[Back](#)

APT Lifecycle





What it is
&
What it is not

What it is not

Advance Persistent Threats (APT) are not like virus attack , which are generic and broad in nature. APT are very specific and bang on target.

Advance Persistent Threats (APT) are not like virus attack which is one time. APT are persistent.

Advance Persistent Threats (APT) are not like virus attack, which may be known and patchable. APT are un patchable and sponsored by a country, organization.


Advance Persistent Threats (APT) are not like spam, malware or virus which may be spontaneous in nature, APT are rational, planned and well coordinated .

Advance Persistent Threats (APT) are not like spam, malware or virus which get detected by Antivirus immediately, APT get detected in months or years.




How to prevent an Organization from Advance Persistent Attack

How to prevent Advance Persistent Attack

- 
1. Sound Policy, Procedure and Guidelines.
 2. Regular (At least once a year) IT Security Audit preferably ISO ISMS 27001
 3. Sound Administrative, Physical and Technical controls.
 4. Configuration Baselineing
 5. User Awareness Training must be conducted at least once a year
 6. Advance Security trainings to IT professionals in the Organization

How to prevent Advance Persistent Attack

- 
7. Good Security Architecture which must include Next Generation Threat Protection (NGTP) instead of traditional Threat Protection.
 8. Signature less Solutions for malware analysis.
 9. Organization must open Security operation Centre (SOC), comprise of SIEM tool to monitor and analysis logs of all system.
 10. Perimeter logical security comprise of sandboxing solutions
 11. By removing Local Administrative privileges from user's workstation accounts and limiting access to only important applications.



Conclusion

Conclusion

- APTs are well planned, well funded and have specific target in mind, and attacker customize and adapt their Tactics, Techniques and Procedures (TTP) to counter target's security and control. APTs traits are as follows-
- Well Organized
- Planned
- Teamwork makes the dream work
- Efficient
- Advance tools along with Remote Access Trojans (RATs)
- Zero Day Exploit, Technical and Social Engineering
- Tenacious
- Focus, Professional, Patience, Goal Oriented

Conclusion-Reports

- Among the targets Govt. and State Utilities are one of them.
- Energy Utilities are among the top 10 targets.
- India is one of the targets.
- Most critical malware RaTs (Remote Access Trojans) are Dark Comet, LV & Gh0stRAT found active in India.
- CnC (Command-and - Control) Servers were found mainly in USA, China, Russia, Germany.
- Internet Explorer (39%), Java (23%), Flash (23%) & Acrobat Reader (15%) are the main contributor for zero day attack.



THANK YOU